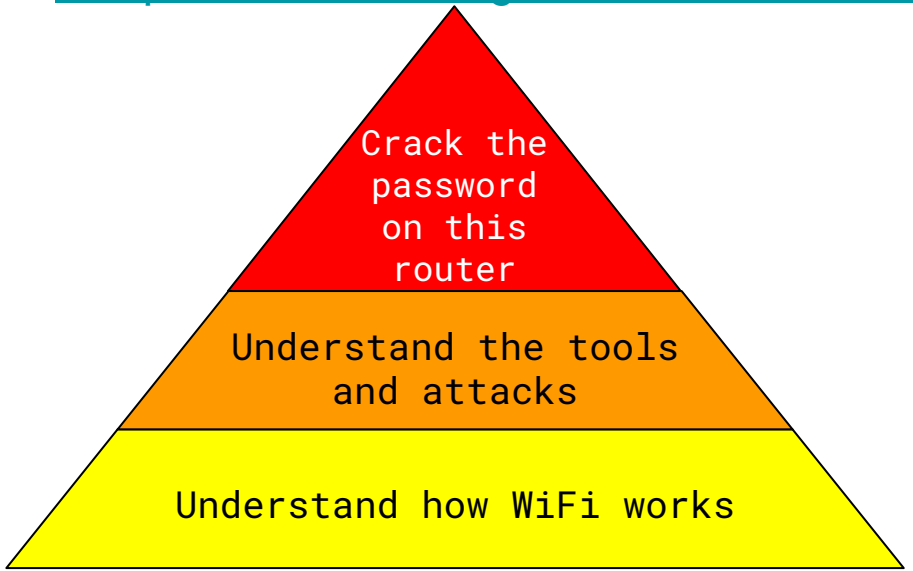
Wi-Fi, Wireshark, and (W)aircrack

An Introduction to Wireless Security

Objective

https://www.netgear.com/home/wifi/routers/r6700/



Outline

1. Setup Stuff (Requirements)
2. What Happens When You Connect To Wi-Fi?
    a. IEEE 802.11 and other Wi-Fi Standards
    b. Joining the Network: Authentication and Association
    c. Wi-Fi Security Protocols
3. Breaking and Entering
    a. Capturing Wi-Fi Handshakes
    b. Attacking Security Protocols

1. Setup Stuff

Linux Systems Required

Requirements

Needed Software:

Wireshark - Packet Analyzer

https://www.wireshark.org/

aircrack-ng - Suite for attacking Wi-Fi networks

https://www.aircrack-ng.org/

sudo apt install wireshark aircrack-ng

Images Courtesy Wireshark Foundation, Aircrack-ng Team

2. What Happens When You Connect To Wi-Fi?

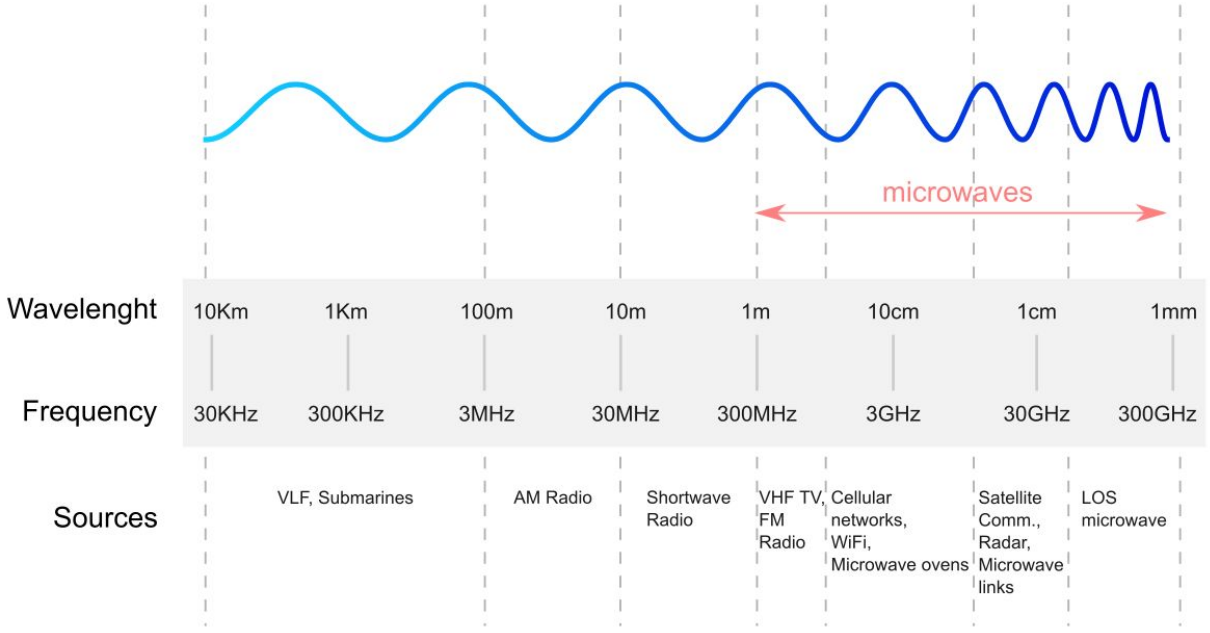
An Introduction to Wi-Fi Protocols

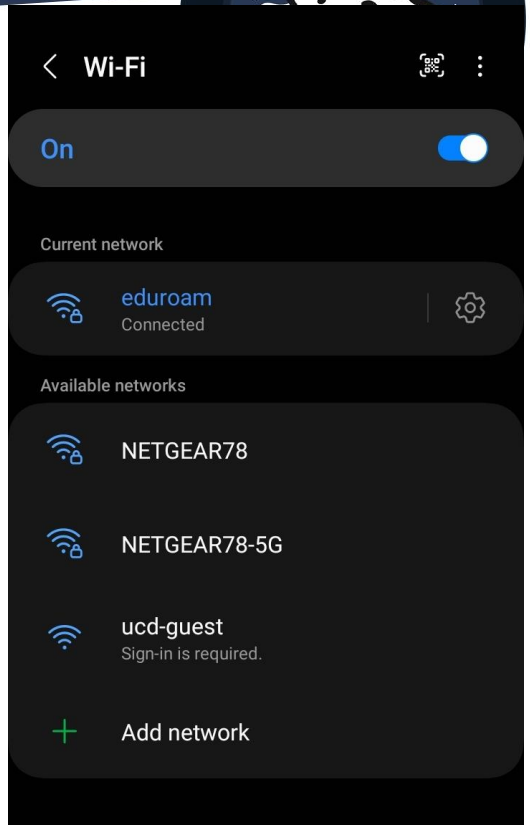
ACT 2,SCENE 1

IEEE 802.11

How does your device “know” what a Wi-Fi network is?

And how does it know how to speak Wi-Fi?


microwaves
Wavelenght
10Km
1Km
100m
10m
1m
10cm
1cm
1mm
Frequency
30KHz
300KHz
3MHz
30MHz
300MHz
3GHz
30GHz
300GHz
Sources
VLF, Submarines
AM Radio
Shortwave Radio
VHF TV, FM Radio
Cellular networks, WiFi, Microwave ovens
Satellite Comm., Radar, Microwave links
LOS microwave


Wi-Fi
On
Current network
eduroam
Connected
Available networks
NETGEAR78
NETGEAR78-5G
ucd-guest
Sign-in is required.
Add network

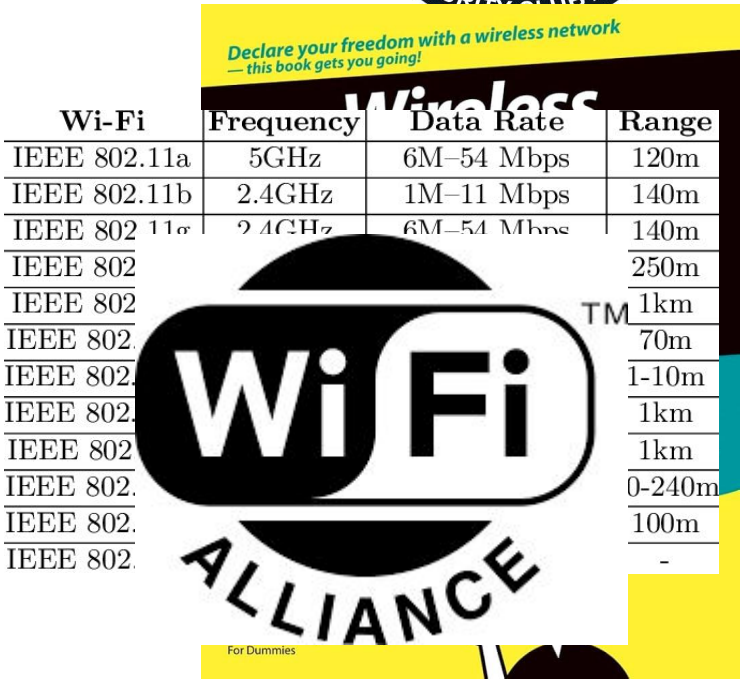
The IEEE 802.11 Standard

“Speaking Wi-Fi For DUMMIES”

- Developed in 1990s by a group at IEEE to standardize wireless networking
- Revised about a dozen times since

Wi-Fi vs 802.11

- Wi-Fi - A brand that guarantees interoperability
- 802.11 - The standard that they work off of



What Does IEEE 802.11 Say?

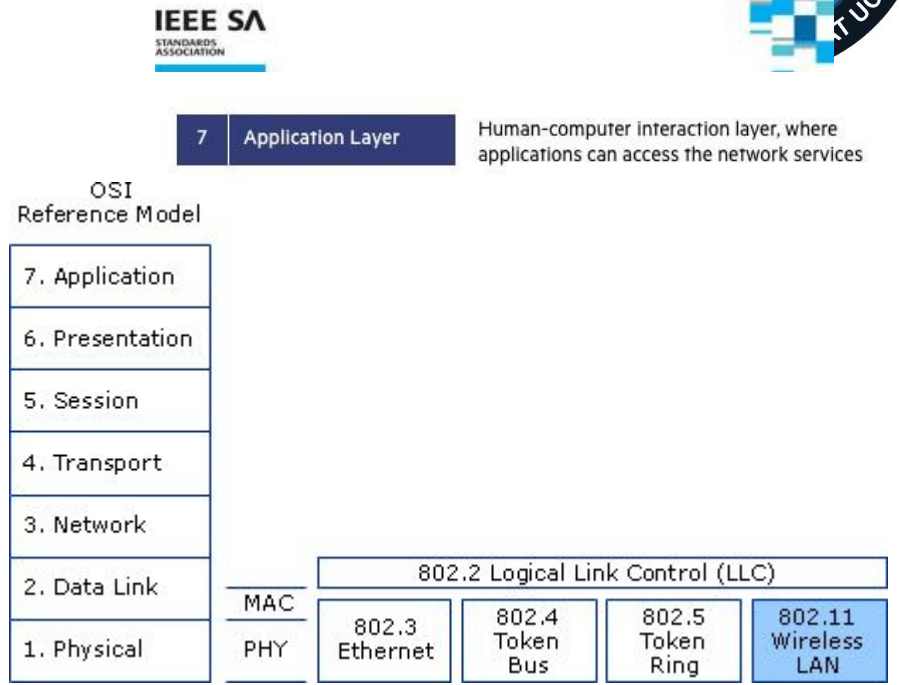
What is 802.11 supposed to do?

- Answer the Who, Where, When, and Hows of wireless communication

Who should be talking?

Where and when should they be talking?

How should they communicate?

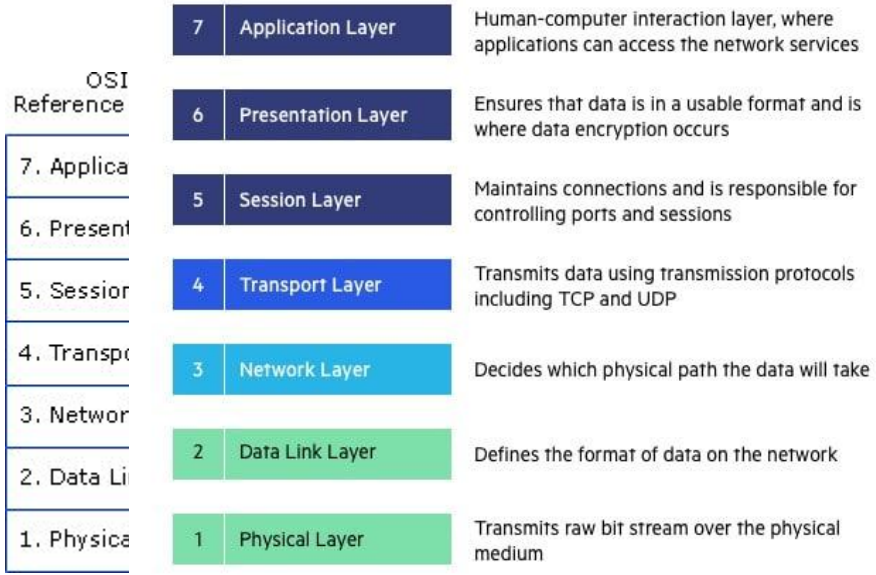


A Brief OSI Detour

OSI Model - A “job description” for network communication protocols

7 “types of jobs” that need to be done

802.11 covers Layer 1 and parts of Layer 2



Who Should Be Talking?

(Wireless) Access Point

- A device that allows you to connect to a network

Client

- A device that connects to and uses the network via the access point

Where Should They Be Talking?

Most Common Frequency Bands:

- 2.4 GHz (slower but better range)
- 5 Ghz (faster but bad range)

These bands are further subdivided into channels.

Channel - A “portion of airwaves” that you can transmit on

#	F_0 (MHz)	Freq ra (M
1	2412	240
2	2417	240
3	2422	241
4	2427	241
5	2432	242
6	2437	242
7	2442	243
8	2447	243
9	2452	244
10	2457	244
11	2462	245
12	2467	245
13	2472	246
14	2484	247

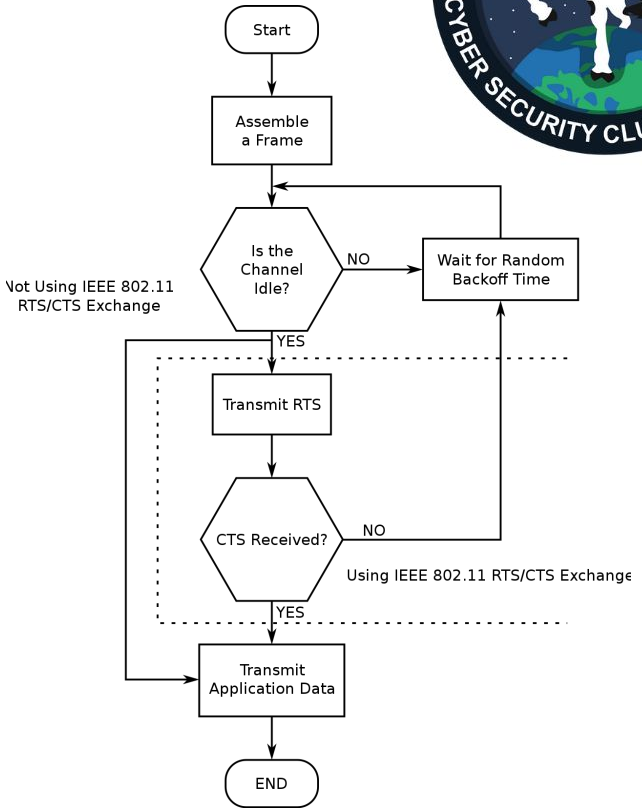
Ch. 20 MHz	F_0 (MHz)	Frequency range (MHz)	F_0 index			US FCC U-NII band(s)	Australia [8]	United States [23]	C [
			40 MHz	80 MHz	160 MHz				
32	5160	5150–5170	✗	✗	✗	U-NII-1	Indoors	Yes	
36	5180	5170–5190	38	42	50				
40	5200	5190–5210							
44	5220	5210–5230	46						
48	5240	5230–5250							
52	5260	5250–5270	54	58		U-NII-2A	Indoors/ DFS/ TPC or[note 5]	DFS/TPC or [note 6]	D
56	5280	5270–5290							
60	5300	5290–5310	62						
64	5320	5310–5330							
68	5340	5330–5350	70	74	82				
72	5360	5350–5370				U-NII-2B			
76	5380	5370–5390	78						
80	5400	5390–5410							
84	5420	5410–5430	86	90					
88	5440	5430–5450							
92	5460	5450–5470	94						
96	5480	5470–5490							
100	5500	5490–5510							

When Should They Be Talking?

If two devices talk on the channel at once, they step on each other.

Carrier-sense Multiple Access with Collision Avoidance (CSMA/CA)

- Process for checking if a channel is “clear” before data is transmitted

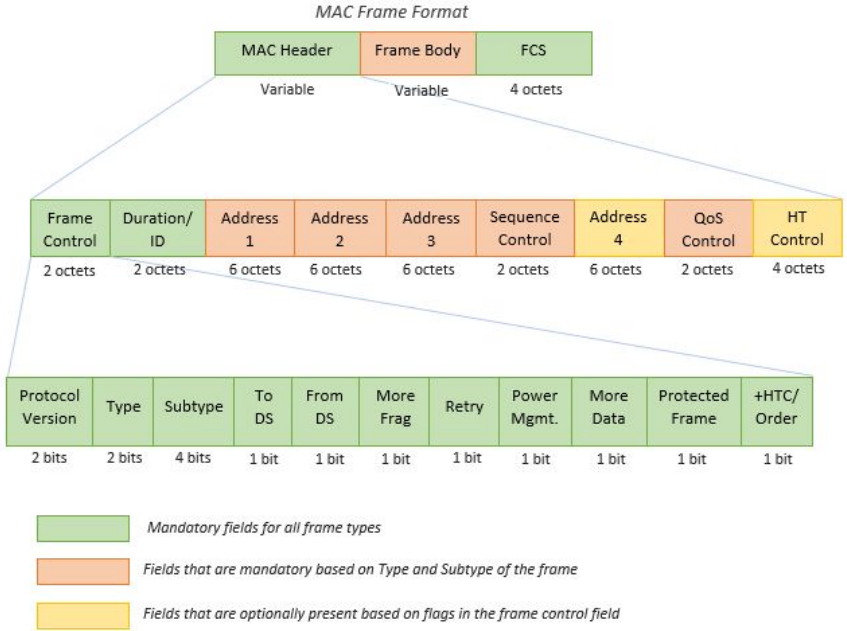


How Should They Be Talking?

802.11 specifies a frame format for all data sent over its networks.

Frame Types of Note:

- Beacon Frame / Probe Response (About Me)
- Deauthentication Frame (Get Off Me Network)
- Frames containing EAPOL data (authentication key data)



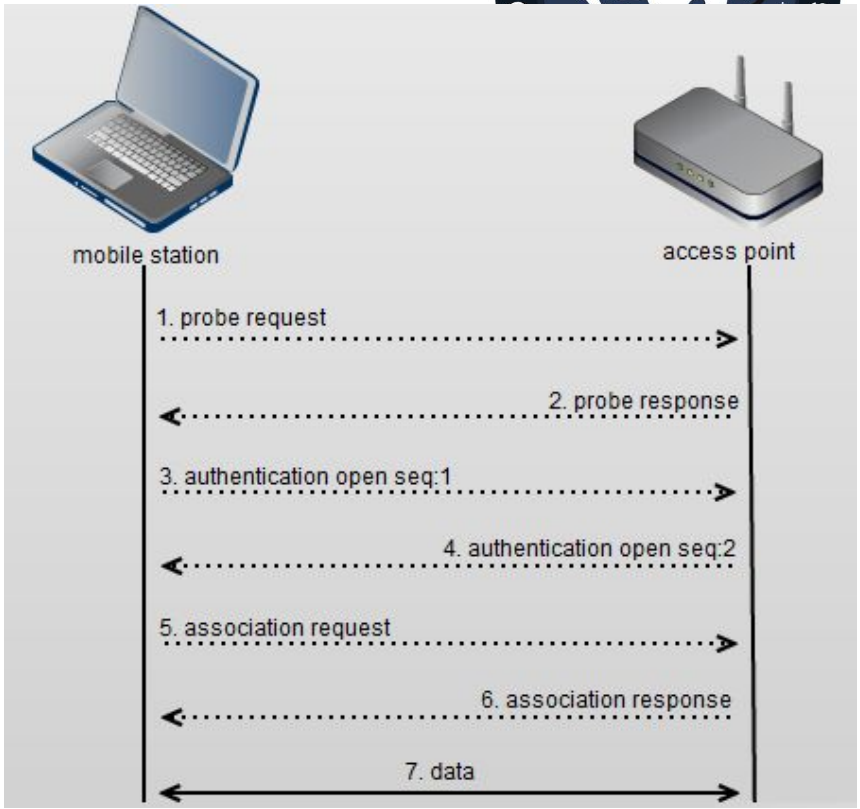
ACT 2,SCENE 2

Shaking Hands

How ***does*** a device connect to Wi-Fi?

The Wi-Fi Connection Process

1) Discovery
    - Probe the network for active APs
2) Authentication
    - WEP - Challenge-Response
    - WPA-series - 4-Way Handshake
3) Association
    - Client picks a specific AP to use to get onto the network



ACT 2,SCENE 3

Good Security, Bad Security

How do you prevent everyone from reading your traffic?

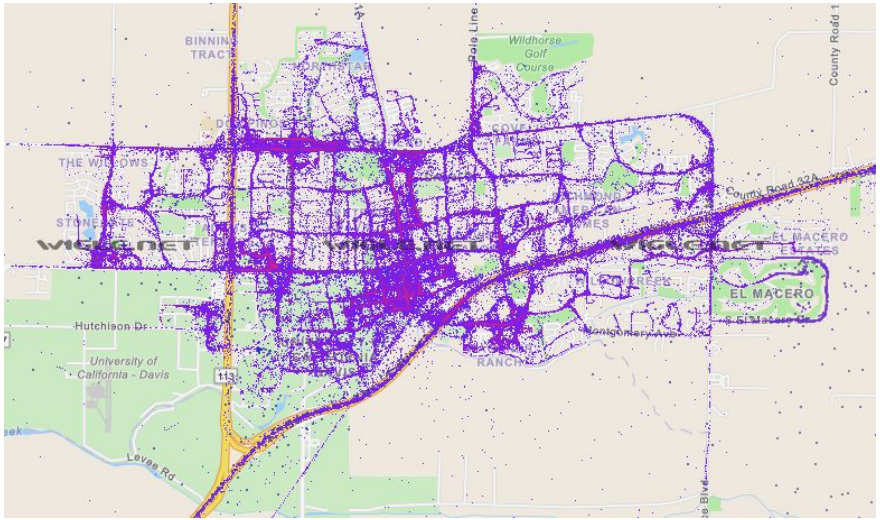
Is it possible to defeat these security measures?

The Problem

How do you prevent someone from reading your traffic if you're just broadcasting it over the air?

Wardriving - Going around collecting info about Wi-Fi networks

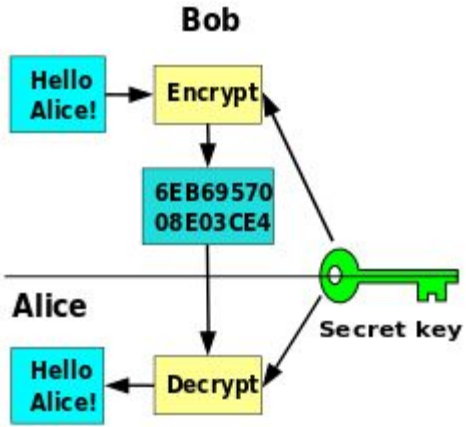
What's stopping me from reading your traffic?



Courtesy wigle.net

The Solution

Encrypt the traffic so that only the intended sender/receiver can read the traffic.



Wi-Fi Encryption

- Wired Equivalent Privacy (1997-2004)
- Wi-Fi Protected Access (2003-2010, in theory)
- Wi-Fi Protected Access 2 (2004-Today)
- Wi-Fi Protected Access 3 (2018-Today, **Current standard)**

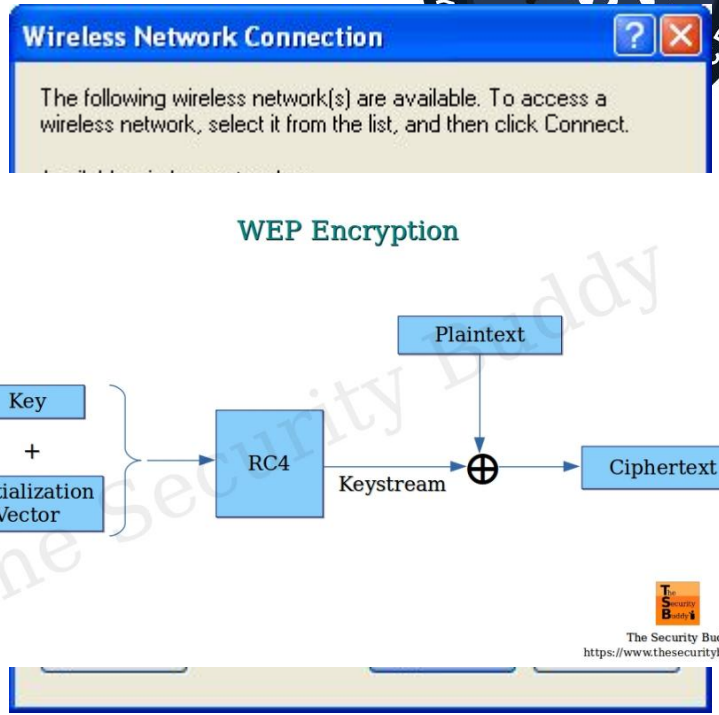
Wired Equivalent Privacy

Part of the original IEEE 802.11 standard

Intended to give “equivalent privacy to being on your own Ethernet wire”

Fixed key and a 24-bit Initialization Vector encrypts the data with RC4

Main vulnerability: Collisions!



Attacking WEP

Issue #1: IV too small, after a while you WILL have a collision and will be able to figure out the key (basic)

Issue #2: The algorithm was implemented badly; you could analyze the keys themselves to recover information

Result: Cracked in **Minutes**!

Wired Equivalent Privacy (**WEP**) is a severely

flawed security algorithm for 802.11

team at the Technische Universität Darmstadt said that they can grab the key with a 95 percent probability of success in as little as two minutes using a 1.7GHz Pentium-M machine to do the calculations.

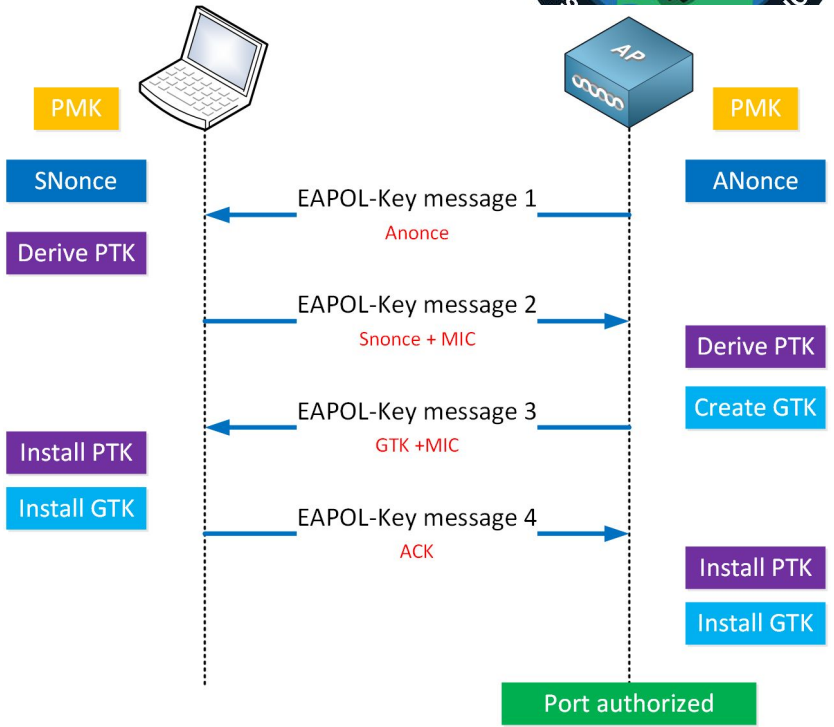
Wi-Fi Protected Access (WPA)

Big change: 256-bit Key now changes with every message (Temporal Key Integrity Protocol)

New Authentication Step: EAPOL and the 4-Way Handshake

A stopgap while WPA2 was developed

Still uses RC4 algorithm, so somewhat more vulnerable

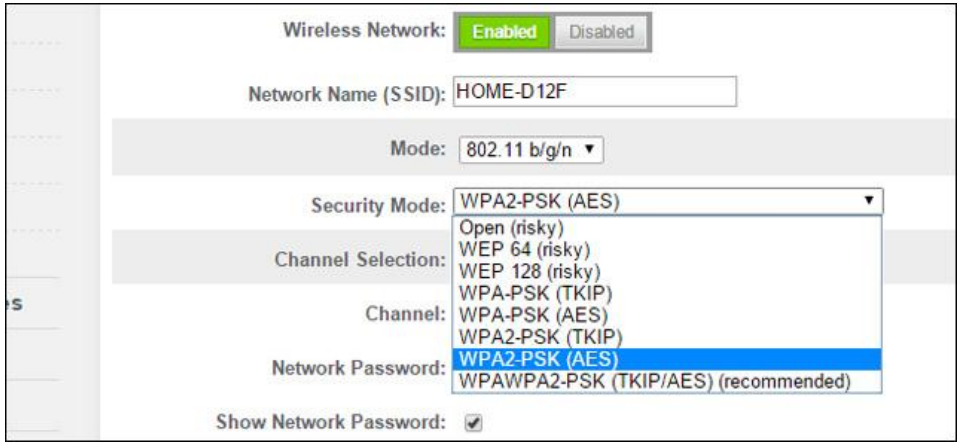


Wi-Fi Protected Access 2 (WPA2)

Better Cipher, Better Security (Papa Johns)

Uses Advanced Encryption Standard (AES) to encrypt data (NSA approved!)

Most devices probably use this protocol



Common Issues to WPA/WPA2

Brute-Forcing Weak Passwords

- If you use a weaksauce password, there's no stopping that

Unsecured Management Frames

- No confirmation between AP and client whether a "disconnect" message is legitimate

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io

Wifi Protected Access 3 (WPA3)

The New Standard in Wi-Fi security

Management Frame Protection
Encrypts management frames so random people can't broadcast them

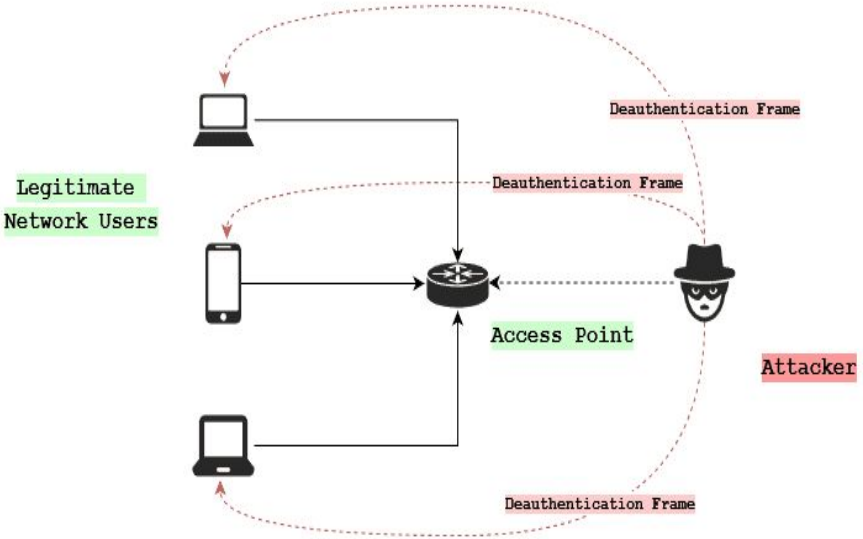
Simultaneous Authentication of Equals / Dragonfly handshake

Uses Zero Knowledge Proofs so that the key exchange isn't transmitted over the air

3. Breaking and Entering

The Plan

1) Set up a network adapter to listen in on the key exchange
2) Capture the packets of the key exchange
3) If we don't get the whole key exchange, deauth the client and wait for them to connect again
4) Crack the weaksauce default password



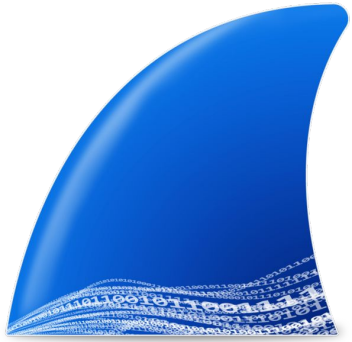
Listening In

Needed:

1) A Wi-Fi adapter with monitor mode capability
2) airmon-ng
3) 1 Nighthawk R6700
4) 1 Volunteer

Steps:

1) Connect the Wi-Fi adapter.
2) ***sudo airmon-ng start wlan0***
3) Boot up Wireshark and start capturing.



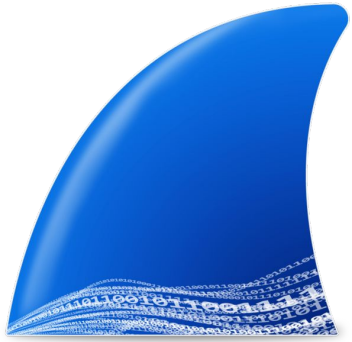
Capture the Packets

Needed:

- Someone to connect to the Wi-Fi
- All 4 EAPOL packets

Protocol	Length	Info
EAPOL	195	Key (Message 1 of 4)
EAPOL	195	Key (Message 2 of 4)
EAPOL	229	Key (Message 3 of 4)
EAPOL	173	Key (Message 4 of 4)

If needed, sort by “eapol” in the search bar



Deauth if Necessary

If you need more packets:

1) Ensure you're on the same channel as the AP
   - *sudo airmon-ng stop*
   - *sudo airmon-ng start wlan0 (channel)*
2) Send deauth frames
   - *sudo aireplay-ng -0 (number of deauth) -a (access point MAC) -c (client MAC) (interface name)*

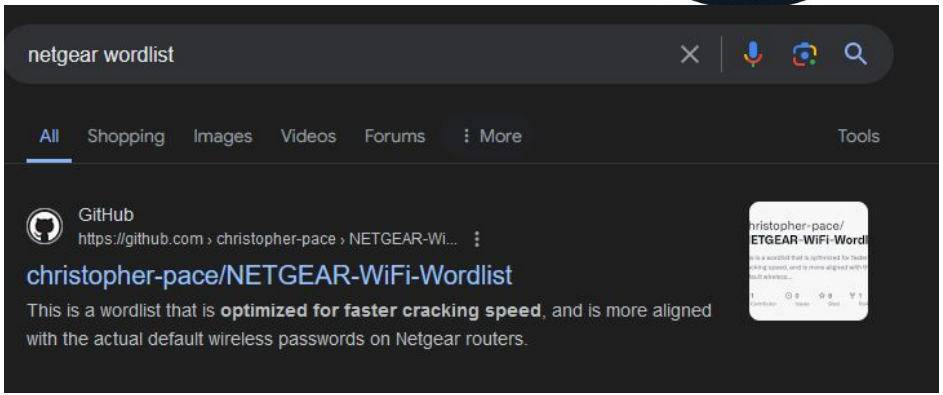
Note:

Your network interface may add a "mon" to the end of its name to indicate it is in monitor mode.

Crack the Password

- Save the captured packets as a PCAP file.
- Find a wordlist.
- Download and extract
  - *gzip -dk (file.gz)*
- Pass it to aircrack-ng

sudo aircrack-ng -b (AP MAC) -w (wordlist) (packet capture file)




```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo aircrack-ng -b A0:63:91:CD:A2:B8 -w 'WoNDeR-List 2014-07-04 6.47mil words.txt.gz' Capture1.pcap
```

What’s the password?

Thank you!

Please change your default passwords.

Special thanks to Zhenkai for providing the Wi-Fi adapter!

Without this, we could not have made this happen.